

Method and Apparatus for Synchronizing Real-Time Clocks of Time Stamping Cryptographic Modules

Field of the Invention

5

The invention relates to time synchronization of an electronic module based system for providing time stamping and cryptographic function. More particularly, the invention relates to an apparatus and method for synchronizing real-time clocks of a plurality of time stamping cipher modules within a same module housing.

10

Background of the Invention

15

The authentication of electronically stored documents is achieving a greater significance in that it is becoming relatively common to exchange electronically stored documents between parties to a transaction. Using digital signatures, it is possible to undeniably determine that the party performing the signature operation is properly authorized to do so. However, if a dispute arises as to what was transmitted as opposed to what was received it may be difficult to establish which version of a document is correct and/or has precedence in time. As a result, many Electronic Document Interchange (EDI) transactions having any monetary significance are normally confirmed with physical documents to provide a paper audit trail. Of course, reducing documents to physical form defeats in large measure the advantages of EDI.

20

25

Accordingly, it is useful to know with certainty the date and time of a digital signature, particularly in the context of electronically maintained diaries, inventor's scientific logs, journals, electronic bids, contracts or the like. One way to resolve this problem is to have all critical documents signed and time stamped by an impartial third party "digital notary" service. Unfortunately, it may be difficult to find such a third party; or it may be difficult to obtain the services in a timely manner. For isolated users, such a digital notary might not be readily available. Moreover, this process may become

30

error-prone, tedious, and a source of bottlenecks, while also creating potential security breaches.

Another solution is to provide in an encrypted form certain data associated with a time and/or a date. Thus the document to be transferred is digitally signed and is time stamped with an encrypted time and date that are associated with the creation of the document. Of course, the integrity of such a method depends critically upon the reliability of the date/time source that is available, for instance a real time clock built into a personal computer or lap-top. Unfortunately, the ability to reset the internal date/time is built into almost all personal computer operating systems, which permits any user to simply set back the clock in their computer and to perform their digital signature operation at an apparently earlier time.

It is known in the prior art to encrypt data for transfer using a time and date obtained from a "trusted clock". U.S. Patent No. 6,105,013 discloses a module for performing secure transactions and digital notary services that includes a continuously running real time clock. The module is designed such that any unauthorized attempt to modify its internal settings will be readily apparent or will result in the deactivation of the module. A service provider initially sets up the module to perform useful functions, such as a priority verification service. The service provider reads the real time clock from each module and creates a module-dependent clock offset object that contains the difference between the reading of the real-time clock and some convenient reference time. The true time can then be obtained from any module by adding the value of the clock offset object to the value obtained from the real-time clock. After some predetermined period of usage, the end-user returns the module to the service provider, pays a fee and receives a new module. Of course, the true time that is obtained from each real time clock can only be trusted to the same extent that the service provider who performed the initial calibration is trusted. The task of calibrating each module separately is an onerous burden on the service provider and may be prone to errors. Further, individual digital clocks are known to vary slightly in dependence upon slight manufacturing inconsistencies and environmental influences. Depending upon the

precision that is desired for a particular application, the unpredictable “clock drift” unique to each module will necessitate more frequent hardware replacements by the service provider.

5 U.S. Patent No 5,001,752 issued to Fischer in 1991 discloses a secure, microprocessor based device embodying a “trusted clock” to countersign important digital signatures by signing them in conjunction with the notarization time taken from the device’s trusted time source. The “trusted clock” is provided with an on-board power source and is packaged in a secure fashion so that the contents of the storage device
10 cannot be externally accessed or observed and so that the clock module cannot be readily tampered with or altered. In a preferred embodiment the device is provided with two “trusted clocks” and a means for comparing the difference between the two clocks with a predetermined threshold value. The two clocks may be used to mutually check each other to ensure neither becomes erratic, thereby extending the period of time during
15 which the clocks may be considered to be “trusted”. If, as a result of clock drift, the time returned by the two clocks differs by an amount greater than the predetermined threshold value, an on-board processor automatically sends a signal to deactivate the unit. Unfortunately, this action requires replacement of the entire module, and a loss of time stamping capabilities during the down-time ensues. It is a disadvantage that it is other
20 than possible for the device to obtain confirmation from an external source to verify that its “trusted clocks” are operating within the predetermined threshold, such that when both clocks drift in a substantially similar manner it is other than possible to detect erratic behavior.

25 U.S. Patent No 5,936,149 issued to Fischer in 1999 discloses an improved token-based device; for instance a device embodied in an MCIA card. The token includes a first and a second real time clock, such that the clocks may be used to mutually check each other to help to ensure neither becomes erratic. Prior to the modules being shipped to an end user, a service provider performs an initialization process. During the
30 initialization process, both notary device clocks accept a current date/time from a master clock having a high degree of accuracy. After a period of time, such as a day or a week,

the notary device is resynchronized with the same master clock and an adjustment factor for correcting the "clock drift" unique to that notary device is retained in the devices permanent memory. A calibrated clock reading may be determined by taking a first clock reading from the master clock, storing the first clock reading, taking a second clock reading from the master clock, storing the second clock reading, and counting the number of oscillations between the master clock readings. Then the actual oscillation frequency may be calculated by using the oscillation count divided by the difference between the second and first master clock readings to compute oscillations per unit time, storing this calculated oscillation frequency and adjusting the output of the on-chip clock device in accordance with the calculated oscillation frequency. The current time after calibration may be computed by the steps of: counting the number of oscillations since the first clock reading (a benchmark time), dividing this value by the calibration value, adding the result to the said first clock reading.

Although U.S. Patent No 5,936,149 discloses an apparatus that provides for internal time correction within a same digital notary module, the device suffers the same limitations of the earlier device disclosed in U.S. Patent No 5,001,752. Specifically, the manufacturer must calibrate separately every module prior to shipping the product to the end user. The clock loading process is only allowed to occur once, such that it is other than possible for the end user to provide the module periodic updates from an external trusted time source, for instance a second module. Further, upon the detection of erratic behavior the module is deactivated, and loss of time stamping function occurs until such time that a new module begins operation. This may, in critically important applications, necessitate that a redundant, back-up module is maintained on-site at all times, resulting in an additional cost to the end user. Still further, the module is designed primarily to address the needs of personal computer and laptop users and does not enable the end user to easily expand a cryptographic system by adding modules. Unfortunately, many operations that are performed by a network server or a computer system of a large corporation require a plurality of such time stamping cryptographic modules working in parallel, each time stamping cryptographic module including a real time clock.

It has now been found that it would be advantageous to provide a time stamping cryptographic module having means for polling other modules that are in electrical communication via a same communications bus. It would be further advantageous to provide a method for performing time-consistency checks between said modules and for providing periodic time value updates to modules that have been identified as other than synchronized with the synchronized modules. According to this method a processing capacity of an existing time stamping cryptographic system may be expanded easily by inserting at least an additional blank module within the same communications bus and establishing electrical communication with at least an existing synchronized module. All necessary time and cipher data is supplied to the new module by the at least an existing synchronized module. Advantageously, as the number of modules within a cryptographic system increases, the overall precision and accuracy of the time keeping devices will also increase.

15 **Object of the Invention**

In an attempt to overcome these and other limitations of the prior art, it is an object of the present invention to provide a system and a method for providing for time consistency checks of modules communicating over very short distances, for instance within a same communication bus.

It is a further object of the present invention to provide a system and a method for automatically disabling unreliable modules.

25 **Summary of the Invention**

In accordance with the invention there is provided a method for updating an on-board clock device to compensate for individual deviation from a time value comprising the steps of:

- 30 a) providing a signal from each of a plurality of modules indicating a time associated with said module and for use by said module in performing time stamping operations;

- b) receiving the signal from each of the plurality of modules and determining a synchronization between the modules to detect synchronized modules and modules that are other than synchronized with the synchronized modules; and,
- c) when a module is detected as other than synchronized with the synchronized modules,
- 5 automatically performing one of synchronizing that module with the synchronized modules and disabling that module from performing timestamping operations.

- In accordance with the invention there is further provided a method for verifying an on-board clock device to compensate for individual deviation comprising the steps of:
- 10 a) receiving a signal including a plurality of time synchronization values at each of a plurality of modules; and
- b) each module determining a synchronization status of itself and, upon determining a status other than in synchronization with the other modules, disabling itself.

- 15 In accordance with the invention there is further provided a method for inserting a new time stamping cryptographic module within an existing cryptographic system comprising the steps of:
- a) installing a module within a communication bus;
- b) detecting the module; and
- 20 c) synchronizing the module by setting the real time clock of the module in dependence upon a value indicative of a current time from the real time clocks of other modules, wherein the step of detecting the module is performed in response to the module providing a signal indicative of a non-synchronized status of the module.

- 25 In accordance with the invention there is further provided a time stamping cryptographic module comprising: a real time clock for providing a time measurement for time stamping functions; a microprocessor connected to the real time clock for handling at least a processing function for periodically updating the real time clock; a secure port in electrical communication with the microprocessor for exchanging information with a
- 30 device external to the module, wherein the secure port is for mating with a corresponding port of a secure communication bus to provide a secure communication channel for

exchanging a value which is characteristic of a time of day with a second other module mated with a second other corresponding port of a same secure communication bus for at least a same overlapping period of time; and, a lock for enabling the module in a first state and for disabling the module in a second other state.

5

In accordance with the invention there is further provided a time stamping cryptographic module comprising: a real time clock for providing a time measurement for time stamping functions; a microprocessor connected to the real time clock for handling at least a processing function for periodically updating the real time clock; a secure port
10 in electrical communication with the microprocessor for exchanging information with a device external to the module, wherein the secure port is for mating with a corresponding port of a secure communication bus to provide a secure communication channel for exchanging a value which is characteristic of a time of day with a second other module mated with a second other corresponding port of a same secure communication bus for at
15 least a same overlapping period of time; means for setting a time of the real time clock in dependence upon a secured time value received from a second other module; and a tamper detection circuit for detecting unauthorized tampering attempts and for providing a signal in dependence thereon and for deactivating the module in response to the signal indicative of an unauthorized tampering attempt.

20

Brief Description of the Drawings

- The invention will now be described in conjunction with the drawings in which:
- 25 Fig. 1a is a simplified block diagram of cryptographic system connected to a computer system according to the present invention;
- Fig. 1b is a simplified block diagram of cryptographic system within a computer system according to the present invention;
- Fig. 2 is a simplified block diagram of a time stamping cipher module;
- 30 Fig. 3 is a simplified block diagram of a time stamping cipher module with an on-board power source and a tamper detection circuit;

Fig. 4 is a simplified block diagram of a time stamping cipher module with a tamper detection circuit;

Fig. 5a is a simplified flow diagram of a method for performing a self-consistency check routine;

5 Fig. 5b is a simplified flow diagram of another alternative method for performing a self-consistency check routine;

Fig. 5c is a simplified flow diagram of another alternative method for performing a self-consistency check routine;

Fig. 6a is a simplified flow diagram of a method for performing an action in dependence upon detecting a module that is other than synchronized;

Fig. 6b is a simplified flow diagram of another alternative method for performing an action in dependence upon detecting a module that is other than synchronized.

Fig. 7 is a simplified flow diagram of a method for inserting a new time stamping cryptographic token within an existing cryptographic system.

15

Detailed Description of the Invention

While the description of the preferred embodiment of the invention disclosed herein is a specific example in which time stamping cryptographic modules are provided in the form of PCMCIA cards within a same module housing. Numerous adaptations of the invention are possible by modifications to the token configuration, number of tokens and the means for providing communication between the tokens, without departing substantially from the teachings of the invention as set forth below.

25 Referring to Fig. 1 and to Fig. 2, shown is a simplified block diagram of a cryptographic system 2 in communication with a computer system in the form of a network server 1 according to the present invention. A plurality of generic modules 10 are provided for performing cryptographic and time stamping functions. Preferably, the plurality of modules 10 are housed within a same module housing 3, the module housing 30 3 having at least one of a tamper resistant and a tamper evidencing feature to ensure that undetected unauthorized external access to the modules 10 is other than possible.

Additionally, the module housing 3 is preferably maintained in a secure facility, for instance a room to which access is restricted. A secure communication line 4 is for exchanging digital information between the computer system 1 and the cryptographic system 2 for encryption/decryption and time stamping functions. Communication
5 between individual modules 10 of the plurality of modules is via a secure communication bus 6. A secure port 15 of the module 10 is mated with a corresponding port 5 of the secure communication bus 6. Conveniently, the modules 10 may draw power from the secure communication bus 6. Of course, while the present embodiment shows modules 10 inserted within the module housing 3, other modules of differing configurations could
10 alternatively be used. Further, is to be understood that at least some modules of the plurality of modules may be of a first configuration while the remaining modules of the plurality of modules are of at least a second different configuration. The specific configurations of the modules that are utilized in a cryptographic system are determined in dependence upon considerations such as: volume of data traffic expected; desired
15 module functionality; desired level of security; and cost considerations.

Referring to Fig. 1b, a simplified block diagram of generic modules 10 of a cryptographic system 2 within a computer system 1 according to the present invention is shown. In this alternate embodiment, the modules 10 are inserted into an interface 9
20 provided within the computer system. Communication between individual modules 10 of the plurality of modules is via a secure communication bus 6. A secure port 15 of the module 10 is mated with a corresponding port 5 of the secure communication bus 6. Conveniently, the modules 10 may draw power from the secure communication bus 6. Of course the specific configurations of the modules that are utilized in a cryptographic
25 system of the type that is described with reference to Fig. 1b are determined in dependence upon considerations such as: volume of data expected; desired functionality; desired level of security; and cost considerations.

Referring again to Fig. 2, a simplified block diagram of a generic time stamping
30 cipher module is shown generally at 10. The module 10 has a real time clock 12, volatile memory 13 to store cipher data including at least a secure-electronic-key and data

relating to time-keeping functions, a cipher processor **11**, a transceiver **14** and a secure port **15**. Because the module has volatile memory **13** for storing data, removal of the cryptographic module **10** from a power source results in erasure of any cryptographic data and time data stored therein. Advantageously, an unpowered module **10** cannot be removed from the cryptographic system **2** by an unauthorized third party and inserted into a second other cryptographic system to perform unauthorized or fraudulent time stamping or encryption functions. The module **10** also includes an electronic lock for enabling the module in a first state and for disabling the module in a second other state. The electronic lock is preferably a function executable by the cipher processor **11** for disabling a module at least temporarily in dependence upon receiving a signal indicative of a module synchronization status that is other than synchronized with the synchronized modules. Preferably, upon receiving a synchronization signal from at least a synchronized module, the cipher processor **11** performs an un-lock function to enable the module for performing time stamping and cryptographic functions.

Referring to Fig. 3, a simplified block diagram of a time stamping cipher module with an on-board power source is shown generally at **20**. The time stamping module **20** has a real time clock **12**, volatile memory means **13** and a portable power source in the form of a battery **16** dedicated to the cryptographic module **20**, which collectively constitute a non-volatile memory means **13a** to store cipher data including at least a secure-electronic-key and data relating to time-keeping functions, a cipher processor **11**, a transceiver **14**, a secure port **15**, and a tamper detection circuit **17**. The tamper detection circuit **17** is for detecting at least an unauthorized attempt to externally access or observe the contents of the cryptographic module **20**, and for communicating a signal indicative of the unauthorized external tampering to the cipher processor **11**. In response to receiving the signal, the cipher processor **11** typically erases the cipher data stored in the non-volatile memory **13a**, effectively deactivating the module. The definition of tampering includes, but is not limited to, actions such as the unauthorized removal of the entire module **20** from the module housing **3**, any attempts to open the module **20** or any attempts to externally probe the contents of the module **20**. The module **20** also includes an electronic lock for enabling the module in a first state and for disabling cryptographic

functions of the module in a second other state. The electronic lock is preferably a function executable by the cipher processor 11 for disabling a module at least temporarily in dependence upon receiving a signal indicative of a module synchronization status that is other than synchronized with the synchronized modules.

5

Referring to Fig. 4, a simplified block diagram of a time stamping cipher module with a tamper detection circuit is shown generally at 30. The time stamping module 30 has a real time clock 12, non-volatile memory 18 to store cipher data including at least a secure-electronic-key and data relating to time-keeping functions, a cipher processor 11, a transceiver 14, a secure port 15, and a tamper detection circuit 17. The tamper detection circuit 17 is for detecting at least an unauthorized attempt to externally access or observe the contents of the cryptographic module 30, and for communicating a signal indicative of the unauthorized external tampering to the cipher processor 11. In response to receiving the signal, the cipher processor 11 typically erases the cipher data stored in the non-volatile memory 18, effectively deactivating the module. The definition of tampering includes, but is not limited to, actions such as the unauthorized removal of the entire module 30 from the module housing 3, any attempts to open the module 30 or any attempts to externally probe the contents of the module 30. The module 30 also includes an electronic lock for enabling the module in a first state and for disabling cryptographic functionality of the module in a second other state. The electronic lock is preferably a function executable by the cipher processor 11 for disabling a module at least temporarily in dependence upon receiving a signal indicative of a module synchronization status that is other than synchronized with the synchronized modules. Optionally, upon receiving a synchronization signal from at least a synchronized module, the cipher processor 11 performs an un-lock function to enable the module for performing time stamping and cryptographic functions.

The time stamping cipher modules previously described with reference to Figs. 2 to 4 are preferably embodied in a secure device, for instance a PCMCIA card. In operation, the modules are preferably kept at a secure facility within a module housing 3 of a cryptographic system 2, usually a peripheral device in communication with a

computer system 1, such as a PCMCIA card reader. Each module is provided with a means for communicating with each of the other time stamping cipher modules within a same module housing 3, for instance, the secure port 15 of each module is mated with a matching port 5 of a secure communications bus 6 within a same module housing 3.

5 Since communication delays along such a communications bus are on the order of a few nanoseconds, and time stamping precision on the order of microseconds or even milliseconds is typically required, communication between modules inserted within a same communications bus are considered to be approximately instantaneous. Note that if communication between modules is internal to the module housing 3, then there is a very
10 high degree of security and the possibility of external “man in the middle” attacks is precluded.

Referring to Fig. 5a, a method for performing a periodic time-consistency check of the “trusted clocks” of a plurality of modules inserted within a same module housing is
15 shown. In the current embodiment a first module is designated as a master module for co-coordinating the time-consistency routines. For instance, the master module is one of the modules inserted in a first position of the secure communication bus 6. Preferably it is the module with the highest level of cryptographic security and the module previously designated as such by a system operator. The master module receives a signal at step 500
20 to initiate a time-consistency check. The master module establishes communication with every other module inserted in a same communication bus at step 501, and authenticates said other modules. Authentication 502 of a module involves determining at least an initialization status and a unique identification for that module. Modules that cannot be authenticated at step 502 are deactivated and an error message is logged to
25 indicate the faulty modules. The master module polls each of the authenticated other modules at step 503 to obtain an on-time point from the real time clock of each module. The master module determines synchronization between the modules at step 504 to detect synchronized modules and modules that are other than synchronized with the synchronized modules. In one embodiment, the master module determines the value of
30 the difference between the time that it registered when the polling signal was sent and the time that each other module registered upon receiving the polling signal. Since

communication between the modules is considered to be approximately instantaneous, each of the values determined by the master module should other than exceed a predetermined tolerance, indicating that all modules are synchronized. Corrections for communication delays over such short distances along a dedicated communication bus
5 are not necessary since the associated delays are at least an order of magnitude smaller than the maximum precision desired for most time stamping functions.

At decision step 505 the master module initiates a predetermined response at step 506 in dependence upon detecting at least a module that is other than synchronized with
10 the synchronized modules. The predetermined response is in dependence of at least the level of security that is maintained for a particular cryptographic system. If the level of security is deemed to be substantially low then the predetermined response may include a routine for updating the real time clock(s) of a module that is other than synchronized with the synchronized modules. If the level of security is deemed to be substantially
15 high, then the predetermined response may be to deactivate and isolate the module that is other than synchronized with the synchronized modules. It will be apparent to one of skill in the art that a log entry indicating at least the predetermined response that was initiated is preferably maintained by the master module for subsequent analysis, for instance during one of routine maintenance and replacement of defective modules.
20 Alternatively, if all modules are synchronized, the master module returns the system to a state of normal cryptographic operation at step 507.

Of course, when the master module is other than synchronized with the synchronized modules, it relinquishes its duties to a second other module within a same
25 module housing. The second other module is designated as a master module according to a predetermined criterion, such as for example the location of the port that it occupies within the communications bus. Once it has been designated as such, the second other module carries out the steps of the routine described with reference to Fig. 5a. The master module is effected according to the method for dealing with modules that are other than
30 synchronized with the other modules.

Referring to Fig. 5b, another method for performing a periodic consistency check between the “trusted clocks” of a plurality of modules contained within a same communications bus is shown. In the current embodiment a first module is designated as a master module for co-coordinating the time-consistency routines. For instance, the master module is one of the module inserted in a first position of the secure communication bus 6, the module with the highest level of cryptographic security and the module previously designated as such by a system operator. The master module receives a signal at step 500 to initiate a time-consistency check. The master module establishes communication with every other module inserted in a same communication bus at step 501. At step 508 the master module performs a combined authentication and polling operation. The operation performed at step 508 includes the action of sending a data packet, for instance a digital document, to each other module of the plurality of other modules. Each other module receives said data packet and encrypts it with a unique identification and with a time stamp using a time and date registered by a real time clock of the module at the time the data packet was received by the module. Each module returns the encrypted and time stamped data packet to the master modules. The master module decrypts the encrypted and time stamped data packet and extracts the unique identification to identify and to authenticate the module originating the packet. Further, the master module extracts the time stamp provided by said other module and compares the time of receipt registered by the other module with the time that was registered by the real time clock of the master module when the original data packet was transmitted. The master module determines synchronization between the modules at step 504 to detect synchronized modules and modules that are other than synchronized with the synchronized modules. In one embodiment, the master module determines the value of the difference between the time that it registered when the polling signal was sent and the time that each other module registered upon receiving the polling signal. Since communication between the modules is considered to be approximately instantaneous, each of the values determined by the master module should other than exceed a predetermined tolerance, indicating that all modules are synchronized. Corrections for communication delays over such short distances along a dedicated communication bus

are other than necessary since the associated delays are at least an order of magnitude smaller than the maximum precision desired for most time stamping functions.

At decision step 505 the master module initiates a predetermined response at step 506 in dependence upon detecting at least a module that is other than synchronized with the synchronized modules. The predetermined response is in dependence of at least the level of security that is maintained for a particular cryptographic system. If the level of security is deemed to be substantially low then the predetermined response may include a routine for updating the real time clocks of a module that is other than synchronized with the synchronized modules. If the level of security is deemed to be substantially high, then the predetermined response may be to deactivate and isolate the module that is other than synchronized with the synchronized modules. It will be apparent to one of skill in the art that a log entry indicating at least the predetermined response that was initiated is optionally maintained by the master module for subsequent analysis, for instance during one of routine maintenance and replacement of defective modules. Alternatively, if all modules are synchronized, the master module returns the system to a state of normal cryptographic operation at step 507.

Of course, when the master module is other than synchronized with the synchronized modules, it relinquishes its duties to a second other module within a same module housing. The second other module is designated as a master module according to a predetermined criterion, such as for example the location of the port that it occupies within the communications bus. Once it has been designated as such, the second other module carries out the steps of the routine described with reference to Fig. 5b.

25

The signal received by the master module at step 500 of the time-consistency routines described with reference to both Fig. 5a and Fig. 5b may be initiated when a predetermined event is indicated, such as the receipt of a digital document to be time stamped, the occurrence of an error within at least a cryptographic module, the detection of a power fluctuation or the detection of external tampering. Of course, it is entirely

30

envisaged that other events either internal to or external to the cryptographic system could also trigger such a signal.

Referring to Fig. 5c, yet another method for performing a periodic consistency check between the “trusted clocks” of a plurality of modules contained within a same communications bus is shown. In the current embodiment a first module is designated as a master module for co-coordinating the time-consistency routines. For instance, the master module is one of the module inserted in a first position of the secure communication bus 6, the module with the highest level of cryptographic security and the module previously designated as such by a system operator. Absent a polling request, the master module receives an unsolicited signal from each module within a same communication bus at step 510. The unsolicited signal preferably is sent to the master module at the expiration of predetermined time intervals at step 509, such as the period of time during which the real time clocks of the modules remain trusted for a specific application. Applications requiring greater time stamping precision have a shorter predetermined time interval compared to applications requiring lower time stamping precision.

The signal indicative of a unique module identification and of a current time of day registered by the real time clock of said module that is sent to the master module at step 510 is preferably a single encrypted and time stamped data packet similar to the one that was returned to the master module at step 508 of Fig. 5b. Absent the polling request from the master module, the data packet is one of a predetermined data packet stored in the memory of the module and a digital document provided previously to the module from the computer system. Of course, other means could also be used to provide a suitable data packet for encryption by the module, such as generating internal to the module at least a random string of alpha-numeric characters. The master module decrypts the encrypted and time stamped data packet and extracts the unique identification to identify and to authenticate the module originating the packet. Further, the master module extracts the time stamp provided by said other module and compares the time of transmission registered by the other module with the time that was registered

by the real time clock of the master module when the data packet was received. The processing time required to time stamp and encrypt the data packet transmitted at step 510 can be precisely determined for each module and added to the actual time registered by the real time clock of that module to further improve precision.

5

Alternatively, the signal indicative of a unique module identification and of a current time of day registered by the real time clock of said module that is sent to the master module at step 510 is a series of two separate signals. The first unencrypted signal includes at least a unique identification for the originating module and an authentication message. The second signal includes at least a same unique identification for the originating module and the exact time that was registered by the real time clock of that module when the first signal was transmitted to the master module. The master module authenticates each other module using the information that was received with the first signal, and additionally determines the exact transmittal time of the first signal from each module using the real time data that was received with the second signal.

10
15

The master module determines synchronization between the modules at step 504 to detect synchronized modules and modules that are other than synchronized with the synchronized modules. In one embodiment, the master module determines the value of the difference between the time that it registered when the data packet was received and the time that each other module registered upon transmitting each unique data packet. Since communication between the modules is considered to be approximately instantaneous, each of the values determined by the master module should other than exceed a predetermined tolerance, indicating that all modules are synchronized. Corrections for communication delays over such short distances along a dedicated communication bus are other than necessary since the associated delays are at least an order of magnitude smaller than the maximum precision desired for most time stamping functions.

20
25

At decision step 505 the master module initiates a predetermined response at step 506 in dependence upon detecting at least a module that is other than synchronized with

30

the synchronized modules. The predetermined response is in dependence of at least the level of security that is maintained for a particular cryptographic system. If the level of security is deemed to be substantially low then the predetermined response may include a routine for updating the real time clocks of a module that is other than synchronized with the synchronized modules. If the level of security is deemed to be substantially high, then the predetermined response may be to deactivate and isolate the module that is other than synchronized with the synchronized modules. It will be apparent to one of skill in the art that a log entry indicating at least the predetermined response that was initiated is optionally maintained by the master module for subsequent analysis, for instance during one of routine maintenance and replacement of defective modules. Alternatively, if all modules are synchronized, the master module returns the system to a state of normal cryptographic operation at step 507.

Of course, when the master module is other than synchronized with the synchronized modules, it relinquishes its duties to a second other module within a same module housing. The second other module is designated as a master module according to a predetermined criterion, such as for example the location of the port that it occupies within the communications bus. Once it has been designated as such, the second other module carries out the steps of the routine described with reference to Fig. 5c.

Alternatively, the above described functions that are performed by the master module during execution of one of the time-consistency check routine described with reference to Figs. 5a to 5c could be performed by all modules of the plurality of modules within a same secure communication bus. Improved reliability for the method of synchronization of the real time clocks would result, but at the expense of increased processing time. Such processor intensive routines could be scheduled to occur less frequently, for instance during off-peak hours. Of course, the verification of synchronization by each module allows for identical module functionality and design, and as such is advantageous in many applications.

Further alternatively, each module may periodically transmit a current time value associated with that module to all other modules of the plurality of modules. Upon receipt of said current time value, all other modules determine independently their synchronization status with the originating module, and return a “vote” of synchronized or other than synchronized with the originating module. The originating module then determines a level of agreement with the other modules, for instance the fraction of other modules that “vote” synchronized. When the determined level of agreement with the other modules is above a predetermined threshold value, the originating module resumes normal cryptographic function. When the determined level of agreement with the other modules is below a predetermined threshold value, the originating module disables itself. Alternatively, the originating module requests a synchronization signal from at least a synchronized module for updating the time value associated with the originating module.

Referring to Fig. 6a, a routine for a predetermined response to be implemented upon the detection of at least a module that is other than synchronized with the synchronized modules is shown. For instance, the predetermined response is initiated at step 506 of one of the time-consistency routines described with reference to Figs. 5a to 5c. The master module, as was previously defined, checks a memory register to determine the time-consistency history of the at least a module that is other than synchronized with the synchronized modules. Preferably, only a predetermined number of most recent time-consistency error log entries are accessed. The predetermined number of the most recent time-consistency error log entries to be considered is determined in dependence upon the level of security that the cryptographic system is assigned. In high security systems, one prior error log entry may constitute a history of erratic behavior. Alternatively, in lower security systems, a threshold number of more than one error log entries must be registered within a predetermined time interval before a module is considered to have a history of erratic behavior.

If a history of erratic behavior for the at least a module that is other than synchronized with the synchronized modules is indicated, the master module deactivates said module at step 605, logs an error message at step 603 providing an indication that

said module was deactivated. Absent the deactivated module, normal cryptographic functions of the cryptographic system 2 are resumed at step 604. Of course when each module provides identical functionality, the module verifies its own behaviour history and reacts accordingly.

5

Alternatively, if a history of erratic behavior for the at least a module that is other than synchronized with the synchronized modules is other than indicated, the master module synchronizes said module at step 602 using a current time from the real time clocks of the synchronized modules. The master module logs an error message at step 603 providing an indication that said module exceeded a predetermined tolerance during the current time-consistency check and time stamping the log entry using a current time obtained from its real time clock. Normal cryptographic functions of the cryptographic system 2 are resumed at step 604, including the functions of the resynchronized module.

10

15

20

Referring to Fig. 6b, an alternate routine for a predetermined response to be implemented upon the detection of at least a module that is other than synchronized with the synchronized modules is shown. The method of Fig. 6b is implemented for cryptographic systems operating with the highest practical level of security. Immediately upon the detection of a module that is other than synchronized with the synchronized modules at step 506, that module is deactivated at step 605 and an error message is logged at step 603 providing an indication that said module was deactivated. Absent the deactivated module, normal cryptographic functions of the cryptographic system 2 are resumed at step 604.

25

30

Referring to Fig. 7 a simplified flow diagram of a method for inserting a new time stamping cryptographic token within an existing cryptographic system is shown. Specifically, if increased demand on the resources of an existing cryptographic system indicates that additional cryptographic modules are required, the system operator can order at least an additional blank module. There is no need to calibrate the real time clocks at the manufacturing facility prior to shipping and to maintain the calibrated time value during transport by supplying an on-board power source. The blank module is

inserted into the existing cryptographic system at step 700, remaining inactive until the next periodic time-consistency check routine is initiated at step 701, typically within a period of time less than several hours duration and more preferably within a period of time less than several minutes duration. During the time-consistency check routine at step 700, the blank module is detected by the master module at step 702, and automatically synchronized with the synchronized modules at step 703. Of course, the master module logs a message at step 704 providing an indication of the time that the blank module was synchronized at step 703, however the log entry will be considered a normal behavior for the purpose of determining a history of erratic behavior for said blank module. Normal cryptographic function continues at step 705 with an expanded cryptographic capacity provided by the additional module that was inserted at step 700.

Alternatively, a module is automatically synchronized with the remaining modules upon initialization of said module. Thus, a newly inserted module is, once initialized, synchronized to other timestamping modules within a same housing.

Advantageously, the current methods and system allows modules within a system to automatically correct their time values. Thus even though the clocks may drift slightly with time, the periodic time-consistency checks and synchronization routines allows all modules to continue to function for long periods of time without being replaced. Such a system maintains a current time that is accurate and precise. Further advantageously, communications that are transmitted between modules via the secure communication bus 6 are essentially instantaneous, rendering the time-consistency and synchronization processes very fast. Since all time-based corrections are performed internal to the secure module housing 3, the possibility of security breaches is also greatly reduced. For instance, it is not necessary to replace modules, or to access an information network or other time-source device that is external to the system in order to perform the periodic time-consistency check and synchronization routine.

Further advantageously, if a module is provided with an on-board power source dedicated to maintaining an initialization status and a time value of a module, removal of that module from the module housing could be authorized, for instance to use the

removed module to synchronize modules in another cryptographic system. Such a method would be implemented following the resetting of all modules within a cryptographic system, for instance as a result of a power failure causing loss of power to the cryptographic system. Alternatively, the method would be implemented to

5 synchronize blank modules inserted in a new cryptographic system that is being brought on-line at another location. Advantageously, new cryptographic systems with time stamping function may be synchronized with an existing module, obviating the need to obtain a synchronized module from a manufacturer.

10 Numerous other embodiments may be envisaged without departing from the spirit or scope of the invention.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2